

FIG. 1A

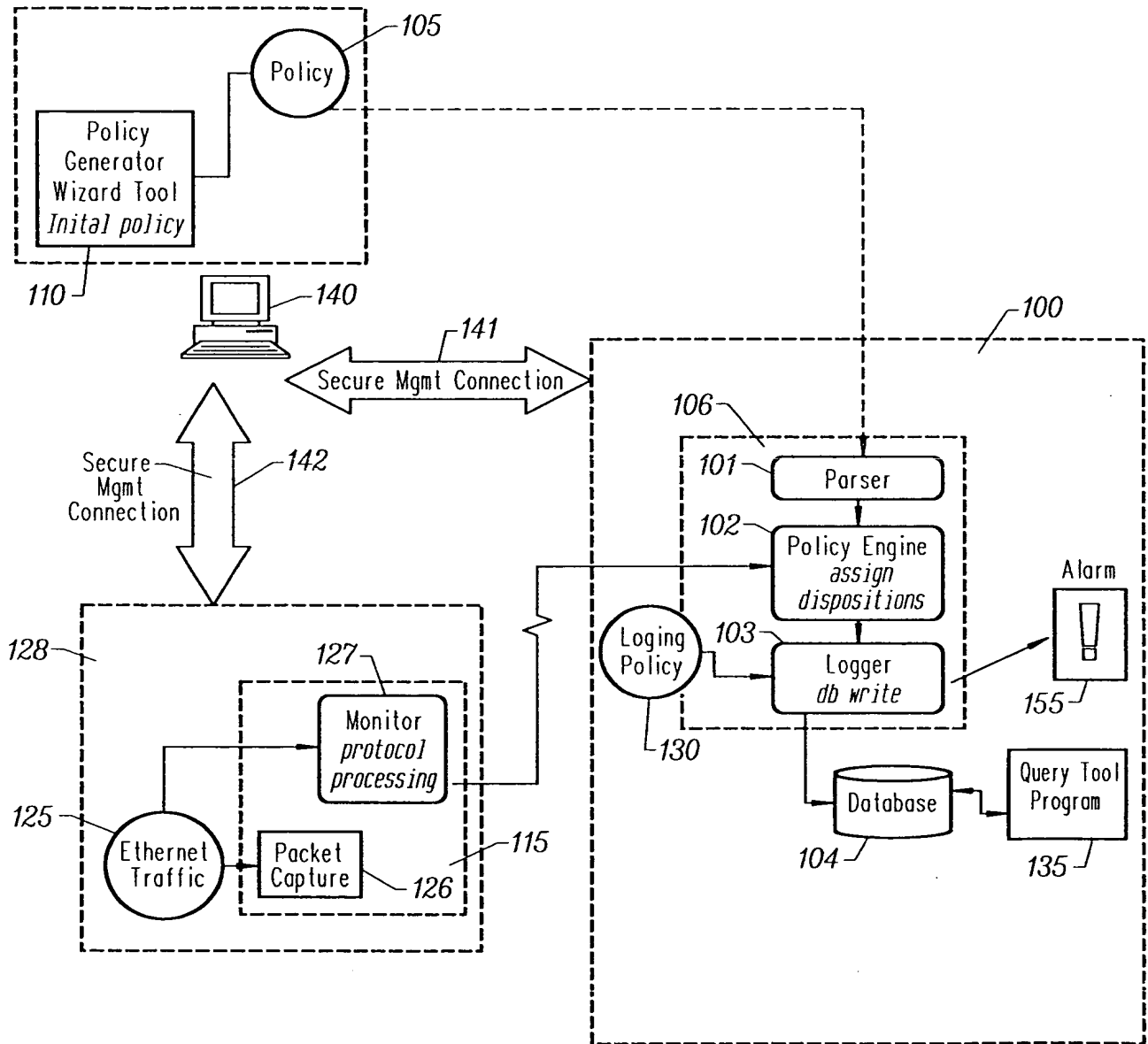


FIG. 1B

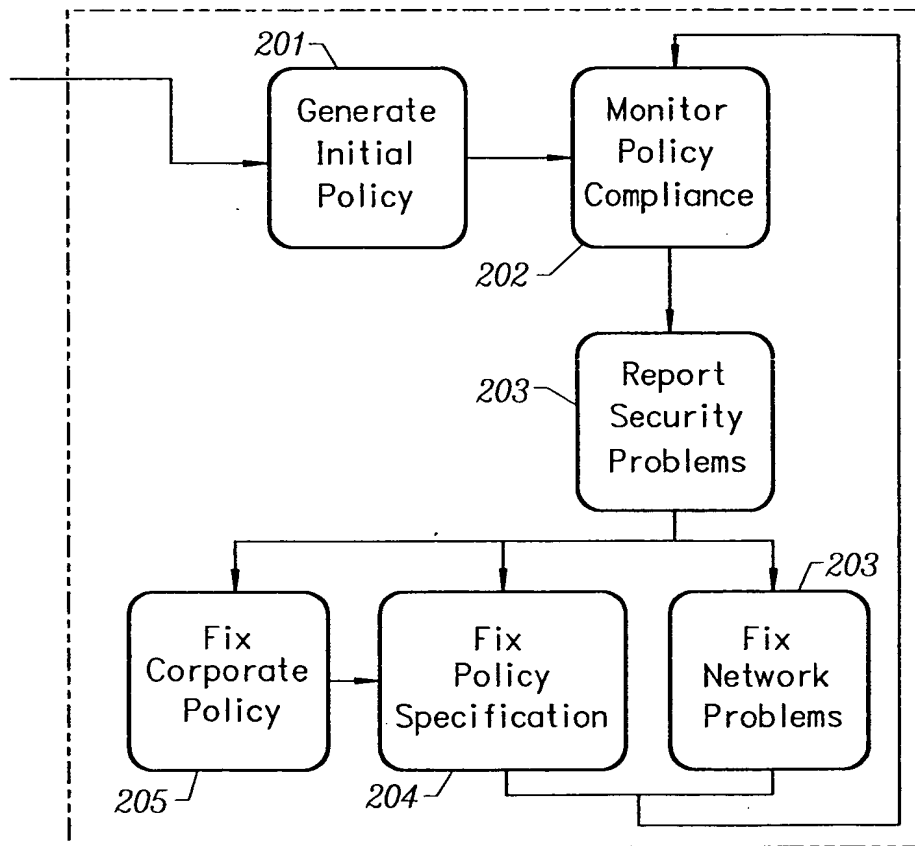


FIG. 2



4/37

301

K Policy Generator

File Help

☐ ☐ ☐ ☐

Community	Policy Domains	Rules	Service	Description	
Name	Includes	Excludes			
Inside_Nodes	10.0.0.0/8			The Hosts in out Intranet	<input type="checkbox"/>
Outside_Nodes		Inside_Nodes		All hosts in the Intranet	<input type="checkbox"/>

☐ New

FIG. 3



5/37

K Policy Processor ✕

Output Director Browse

Output File 402

Process Policy 401

Close

FIG. 4A



6/37

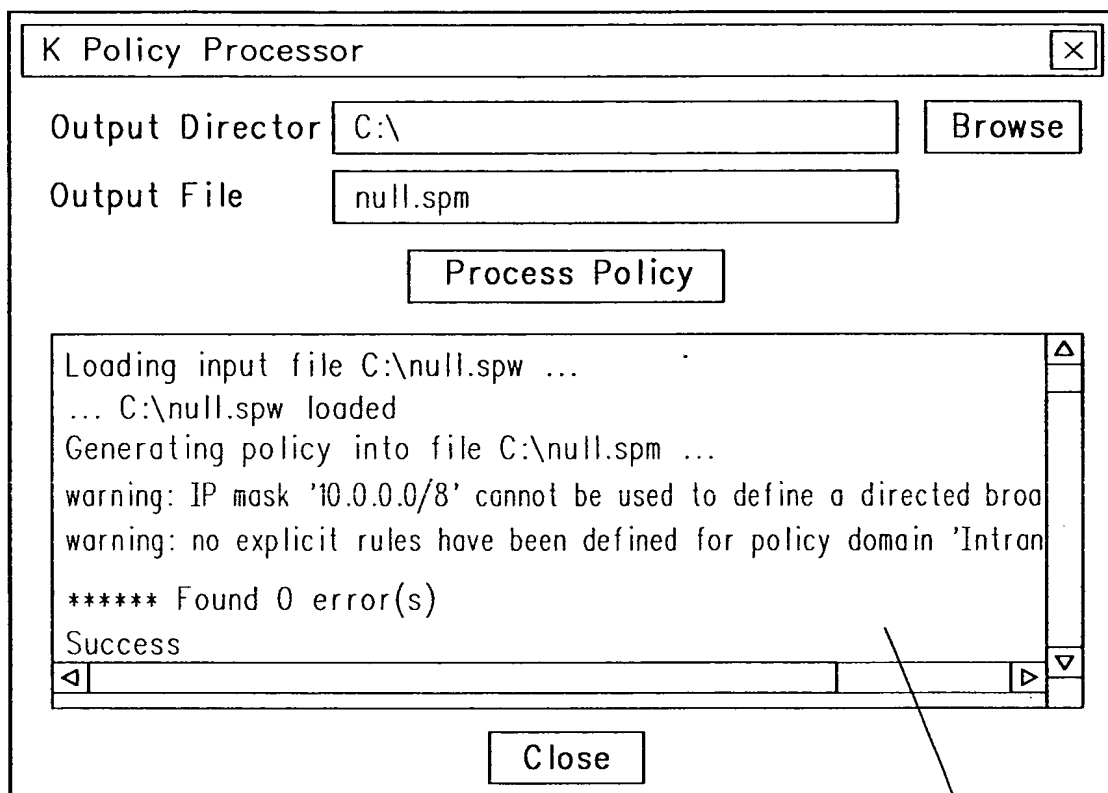


FIG. 4B

SPM: Argument Selector Dialog

Monitor configuration

Input dump file: C:\qs.dmp 501 Browse

Policy: C:\null.spm 502 Browse

Monitornig Point: INTRANET_MONITOR 503
(comma separated)

Monitor Logging Options

Execution Run Comment:

ODBC name: sybase 504

DB Username: policy 505

DB Password: ***** 506 ☒ Save Password [insecure]

Output Options

☐ Output to console:

☒ Output to file: C:\output.txt Browse

Run 507

Exit

Advanced

Help

Progress

nPkts

100%

0%

FIG. 5

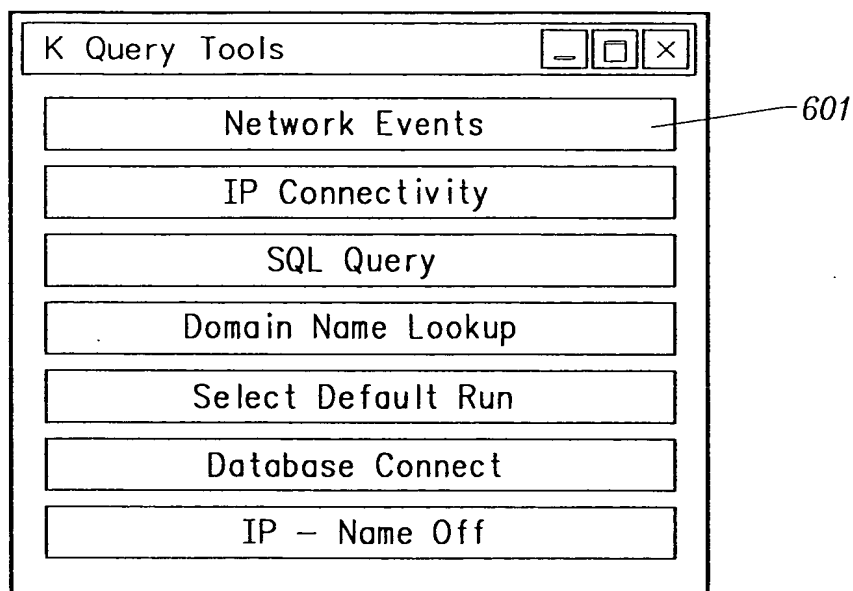


FIG. 6

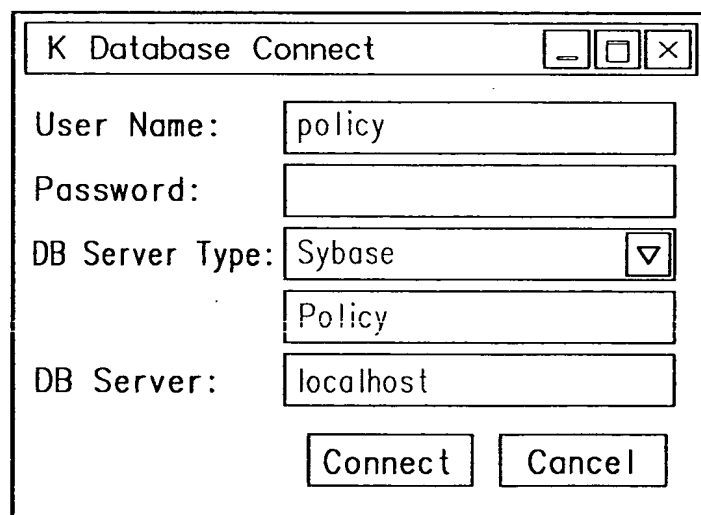


FIG. 7



K Rule View

Execution Run:
1999-10-01 14:30:20.0 C:\.bmp

Final Rule Name:
<Any Rule>

Disposition Name:
<Any Disposition>

Disposition Codes:
☐ Access Denied ☐ Auth Violation ☐ Security Attack ☐ Security QOS ☐ Policy Error ☐ OK

Disposition Severity:
☐ Critical ☐ High ☐ Medium ☐ Monitor ☐ Warning ☐ Information ☐ <none>

Query

Rows

Done

Edit SQL

Copy Row

Copy Deep

FIG. 8



10/37

K Rule View

Execution Run:
1999-10-01 14:30:20.0 C:\.bmp

Final Rule Name:
<Any Rule>

Disposition Name:
<Any Disposition>

Disposition Codes:
☐ Access Denied ☐ Auth Violation ☐ Security Attack ☐ Security QOS ☐ Policy Error ☐ OK

Disposition Severity:
☐ Critical ☐ High ☐ Medium ☐ Monitor ☐ Warning ☐ Information ☐ <none>

Query

Rule Name	Disposition Name	Initiator IP	Init Name	Target IP	Targ Name	Targ Service
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.201		http
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	208.178.27.198		http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	204.71.200.68	www3.yahoo.com	http
Udp_Deny	Udp_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.6	dude.securify.com	domain
Http_Deny	Http_Access_Denied	10.5.63.143	vg-143.securify.com	10.5.63.97	kabale.securify.com	http
Top_Missed_Connections	Warn_Missed_Top_Connect	10.5.63.143	vg-143.securify.com	10.5.63.24	fred.securify.com	netbios-ssn

<

Rows 10

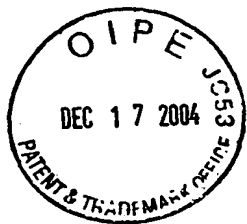
Done

Edit SQL

Copy Row

Copy Deep

FIG. 9



11/37

K Policy Generator	
File Help	
Community	Policy Domains
<div>Policy Domain: <input type="text" value="Intranet"/></div> <div>Identify New or Existing Rule in Intranet</div> <div>Rule Name: <input type="text" value="Internal_Dns"/> <input type="checkbox"/> New <input type="checkbox"/> Delete</div> <div>Add Elements to Internal_Dns</div> <div>Description: <input type="text"/></div> <div><div>Initiators: <input type="text" value="Intranet"/> Inside_Nodes ... Firewall ... Outside_Nodes <input type="button" value="Add Selected"/></div><div>Services: AUTH BOOTP_CLIENT BOOTP_SERVER DNS FINGER <input type="button" value="Add Selected"/></div><div>Targets: Intranet Inside_Nodes ... Firewall ... Outside_Nodes <input type="button" value="Add Selected"/></div></div> <div><div>Initiators: <Any> <input type="button" value="Add Selected"/></div><div>Services: <Any> <input type="button" value="Add Selected"/></div><div>Targets: <Any> <input type="button" value="Add Selected"/></div></div>	

FIG. 10A

K Policy Generator

File Help

Community Policy Domains Rules Service

Select Policy Domain Policy Domain: Intranet

Identify New or Existing Rule in Intranet Rule Name: Internal_Dns New Delete

Add Elements to Internal_Dns Description: Allow DNS to be served from any internal host Set

Initiators: Intranet Inside_Nodes ... Firewall ... Outside_Nodes Add Selected

Services: AUTH BOOTP_CLIENT BOOTP_SERVER DNS FINGER Add Selected

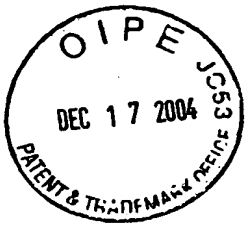
Targets: Intranet Inside_Nodes ... Firewall ... Outside_Nodes Add Selected

Rule Contents for Internet* Dns Initiators: Inside_Nodes Add Selected

Services: DNS Add Selected

Targets: Inside_Nodes Add Selected

FIG. 10B



13/37

K Policy Generator

File Help

Community Policy Domains Rules Service

Name	Includes	Excludes	Description
Inside_Nodes	10.0.0.0/8		The Hosts in out Intranet
Outside_Nodes		Inside_Nodes	All hosts in the Intranet

New

Delete

Find Uses

FIG. 10C

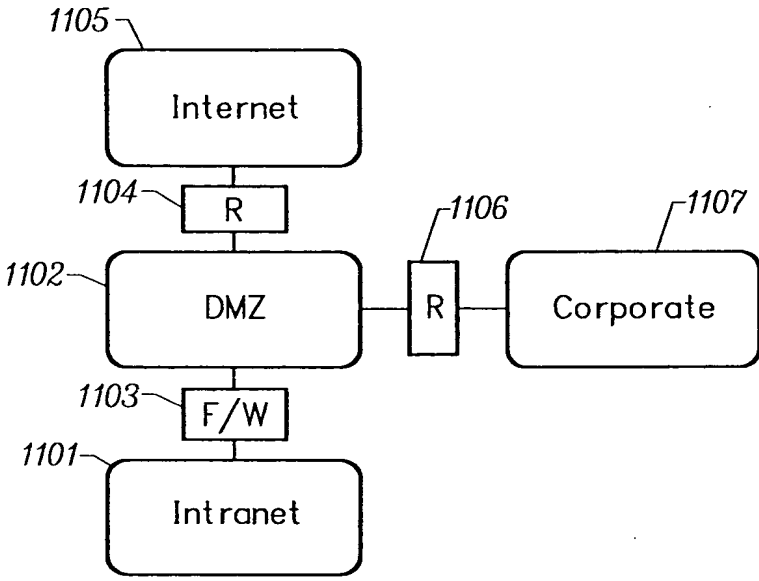


FIG. 11

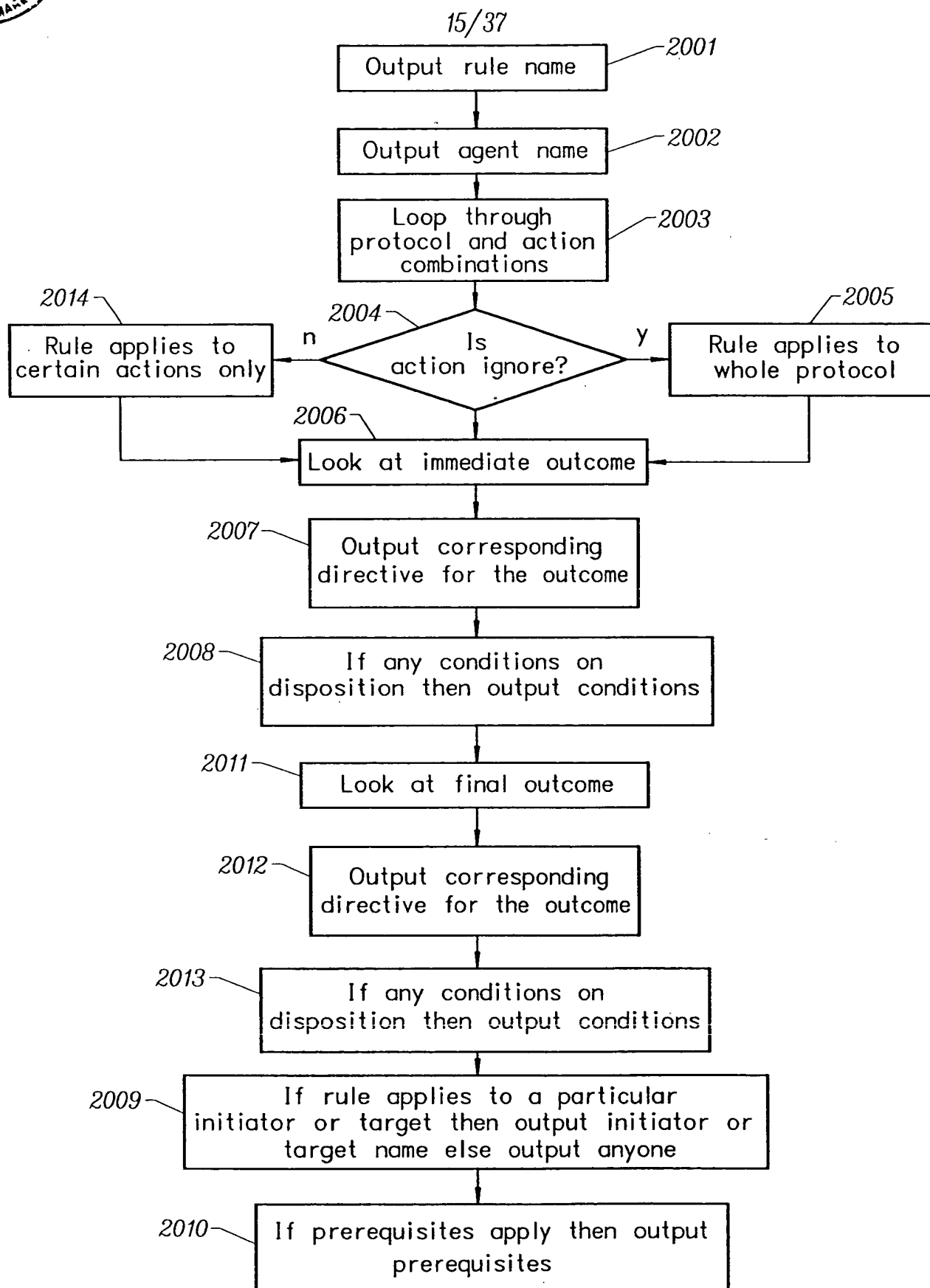


FIG. 12

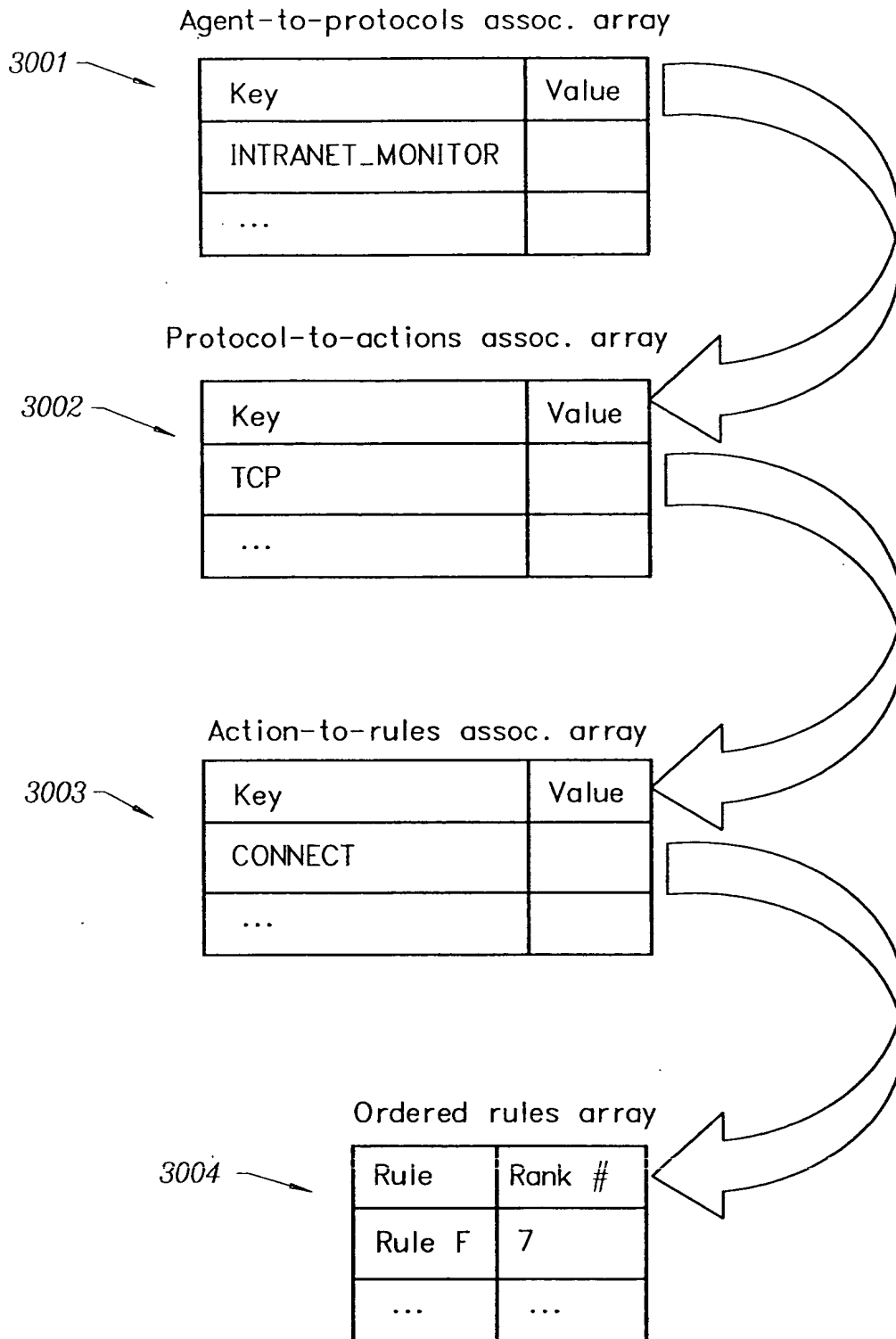


FIG. 13



17/37

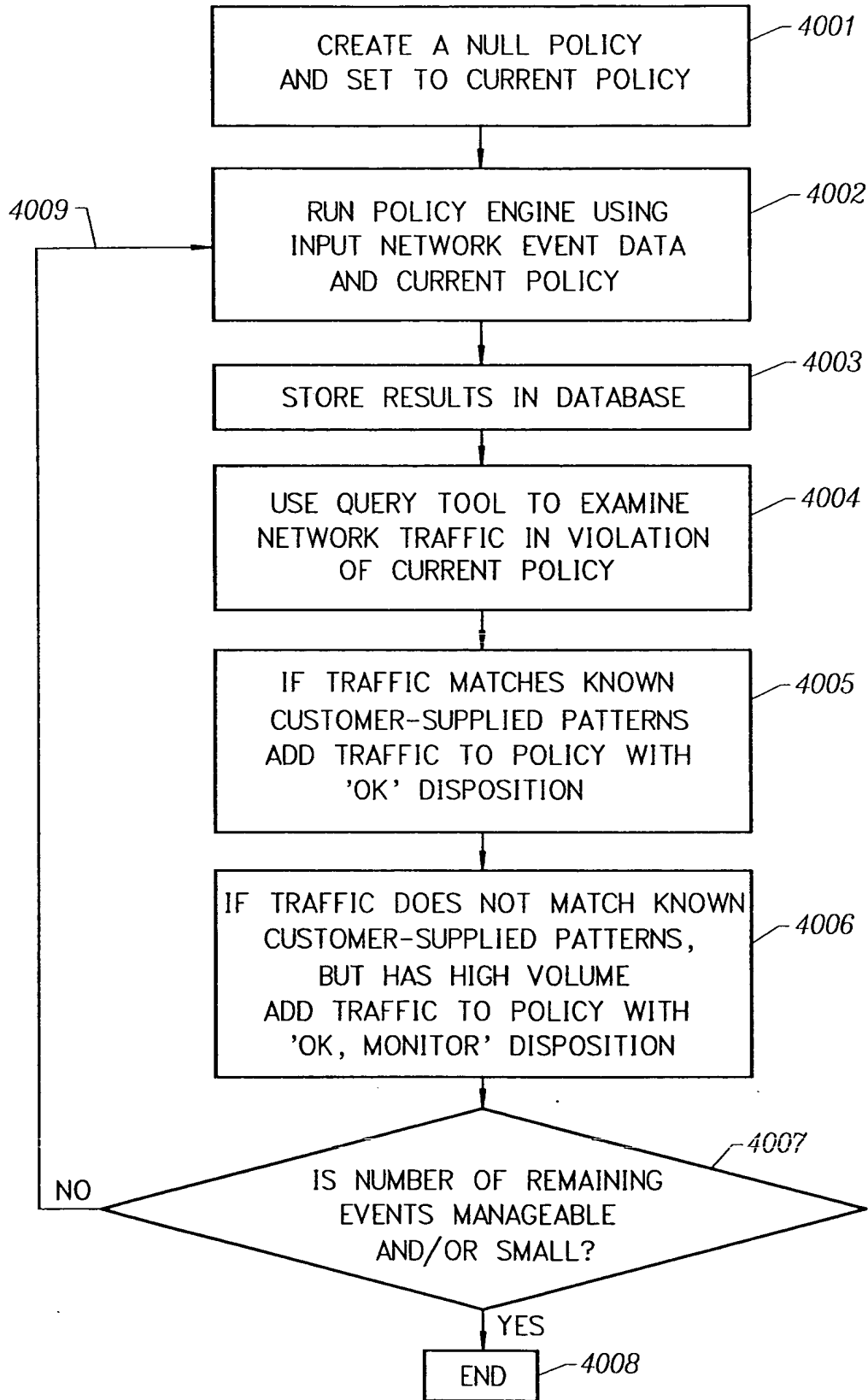


FIG. 14

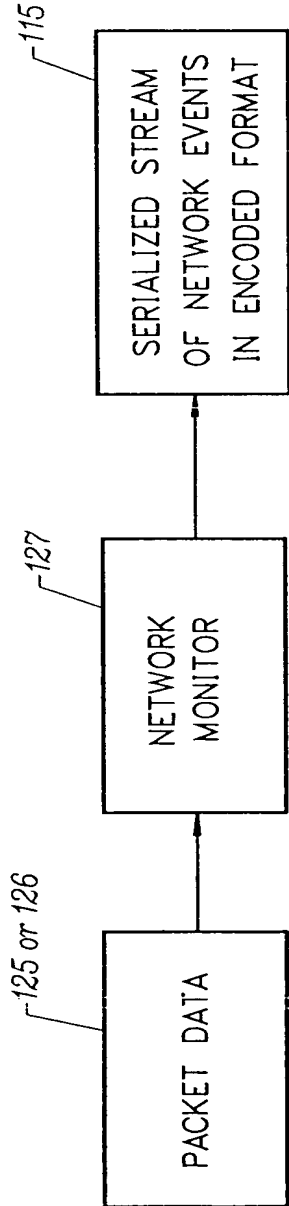


FIG. 15

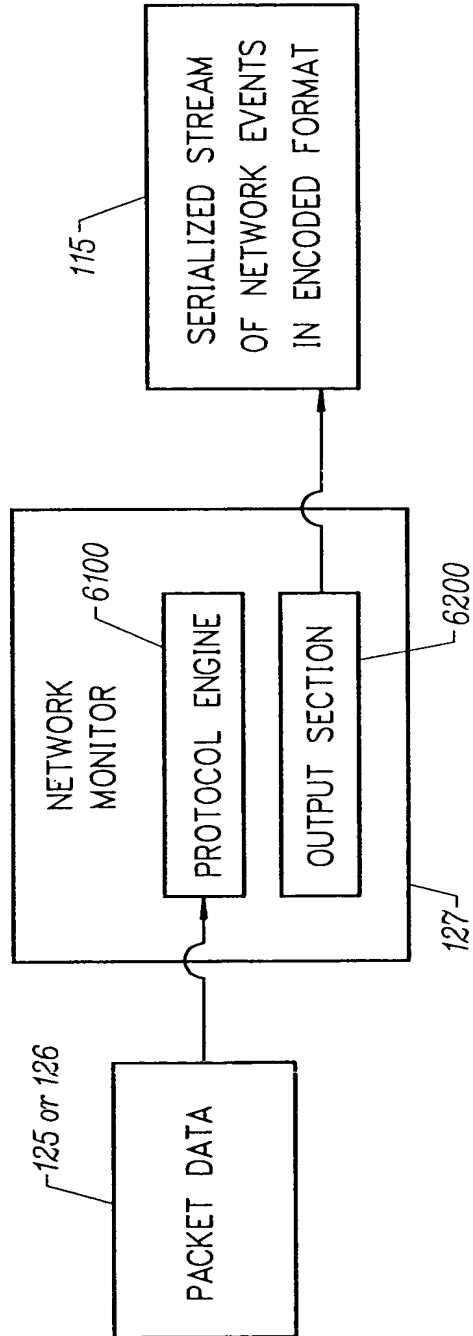


FIG. 16

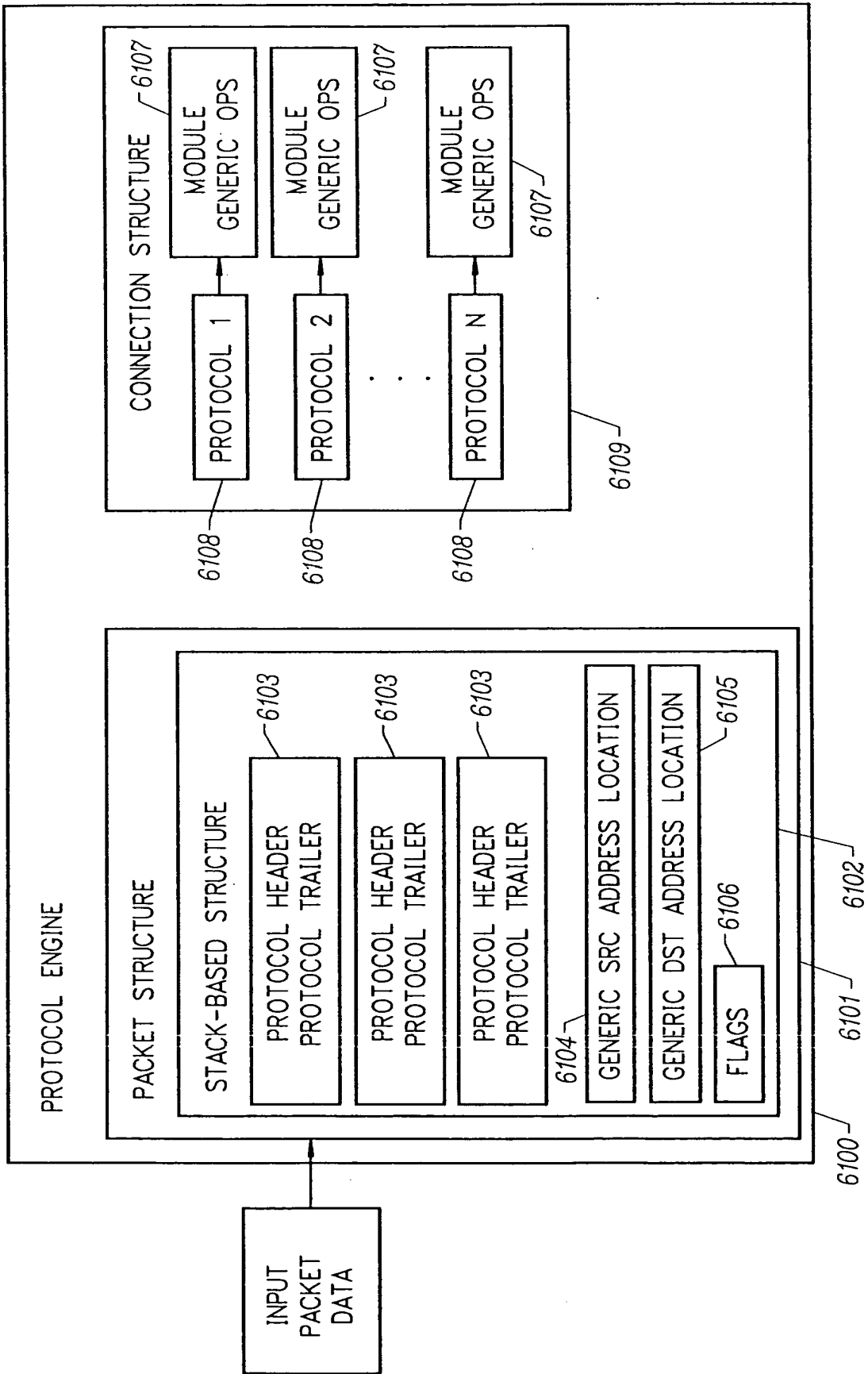


FIG. 17

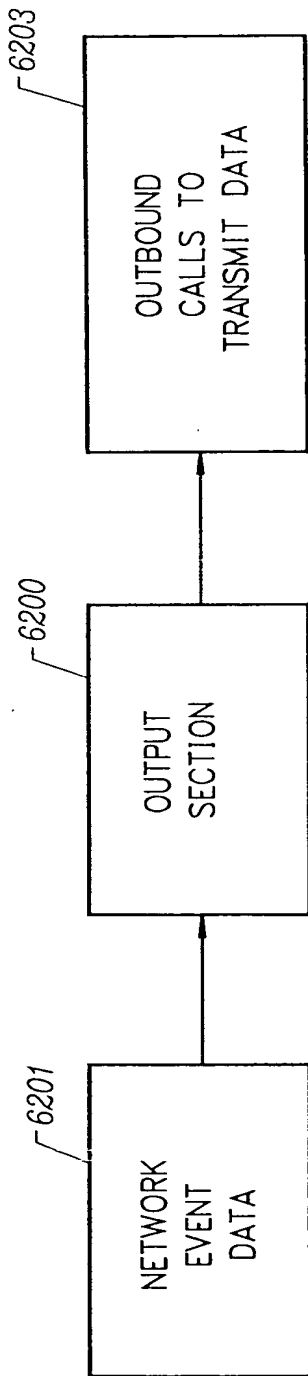


FIG. 18

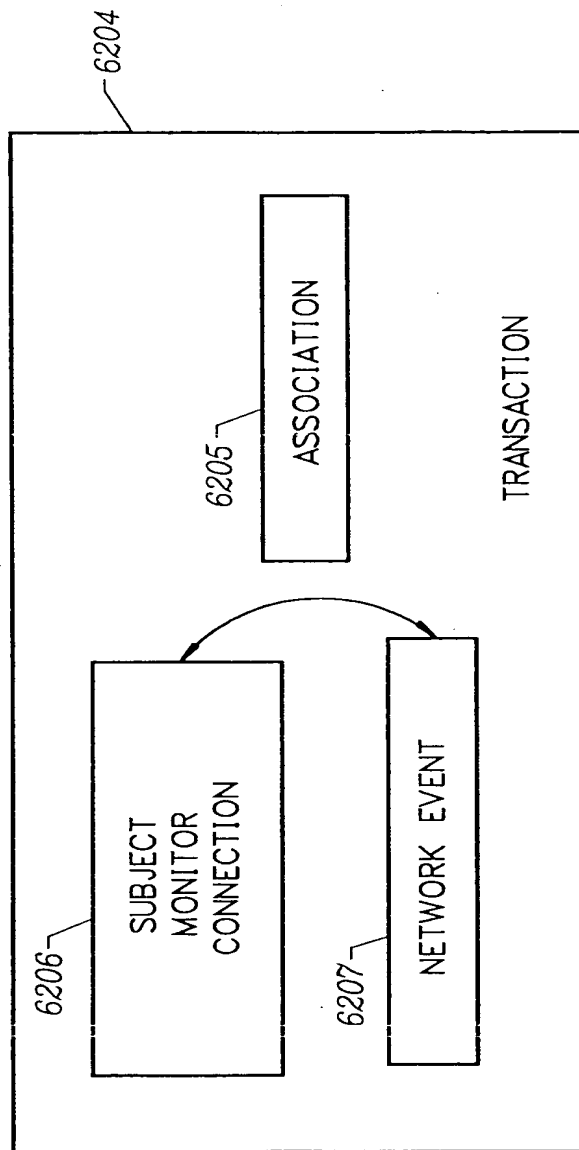
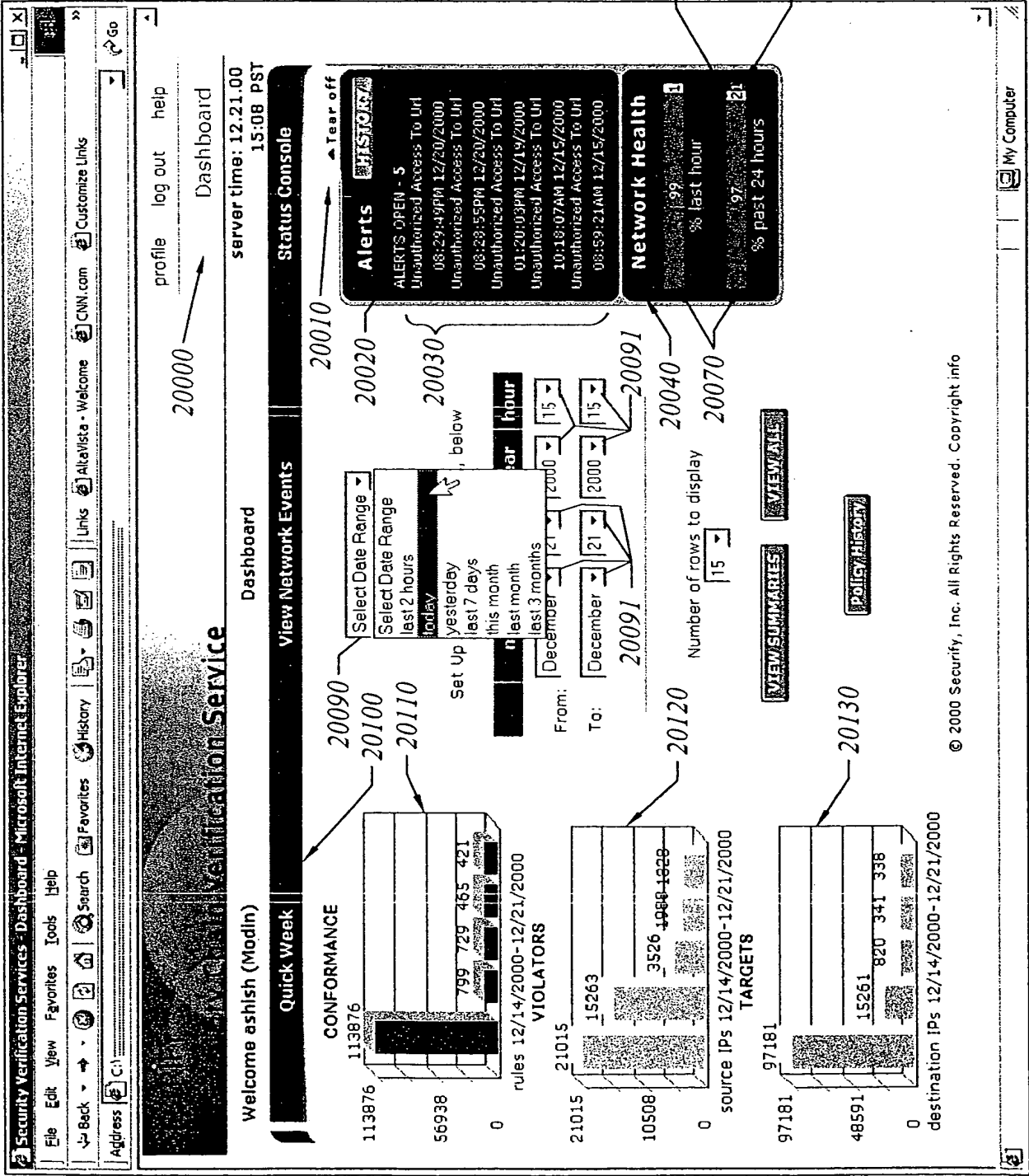


FIG. 19



BEST AVAILABLE COPY

FIG. 20





22/37

BEST AVAILABLE COPY

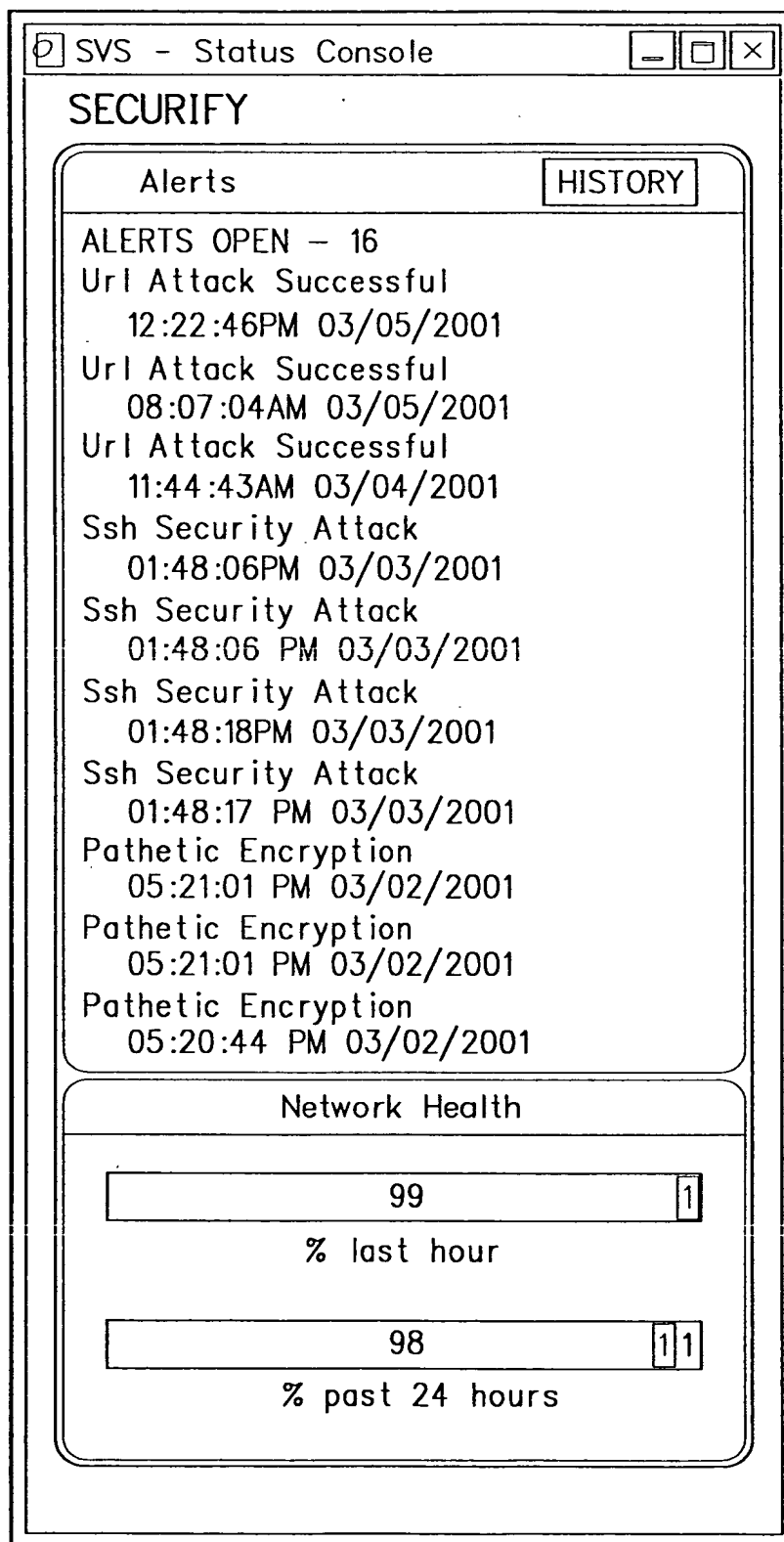
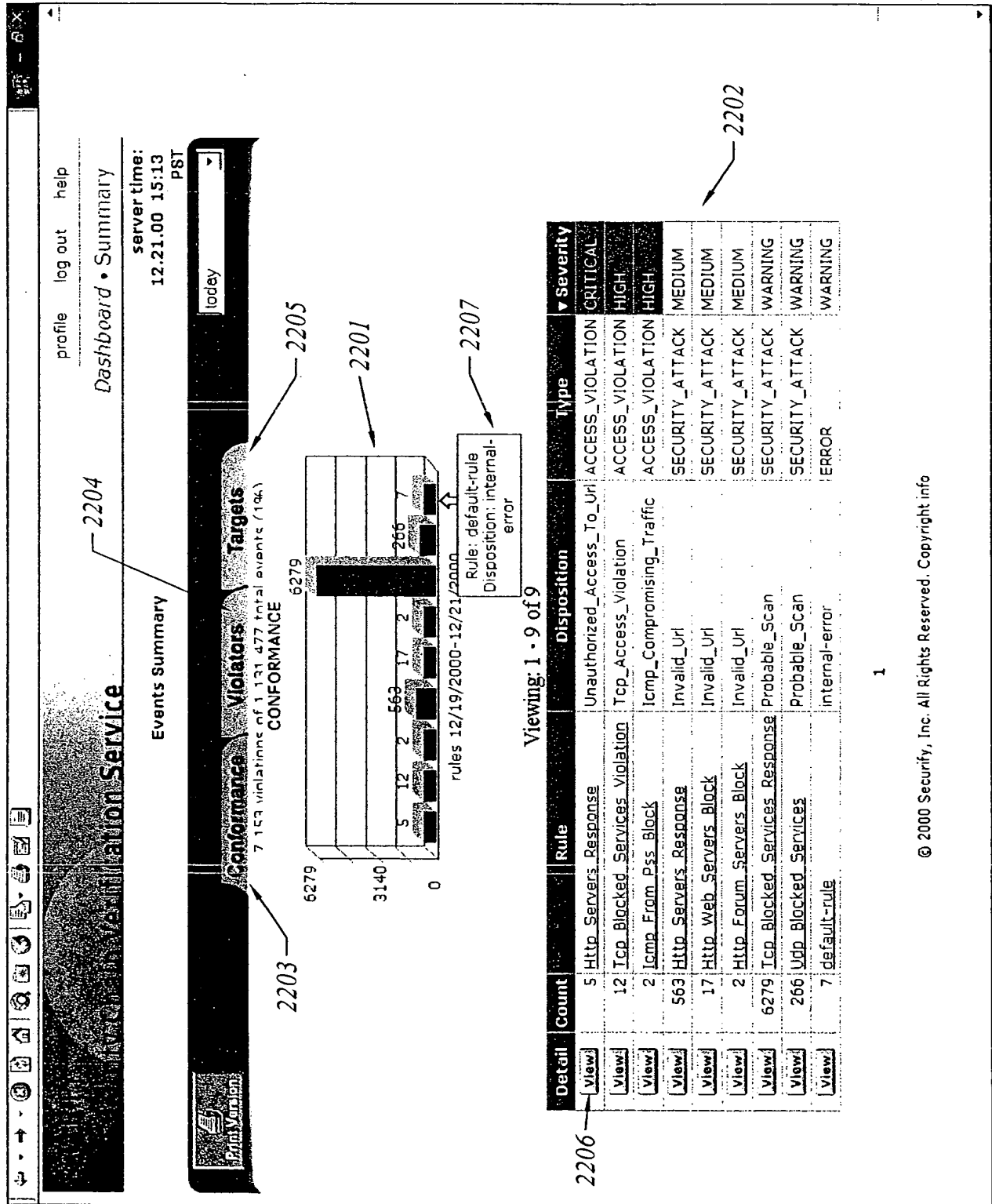
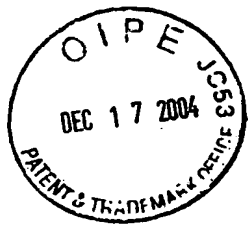


FIG. 21

FIG. 22

BEST AVAILABLE COPY

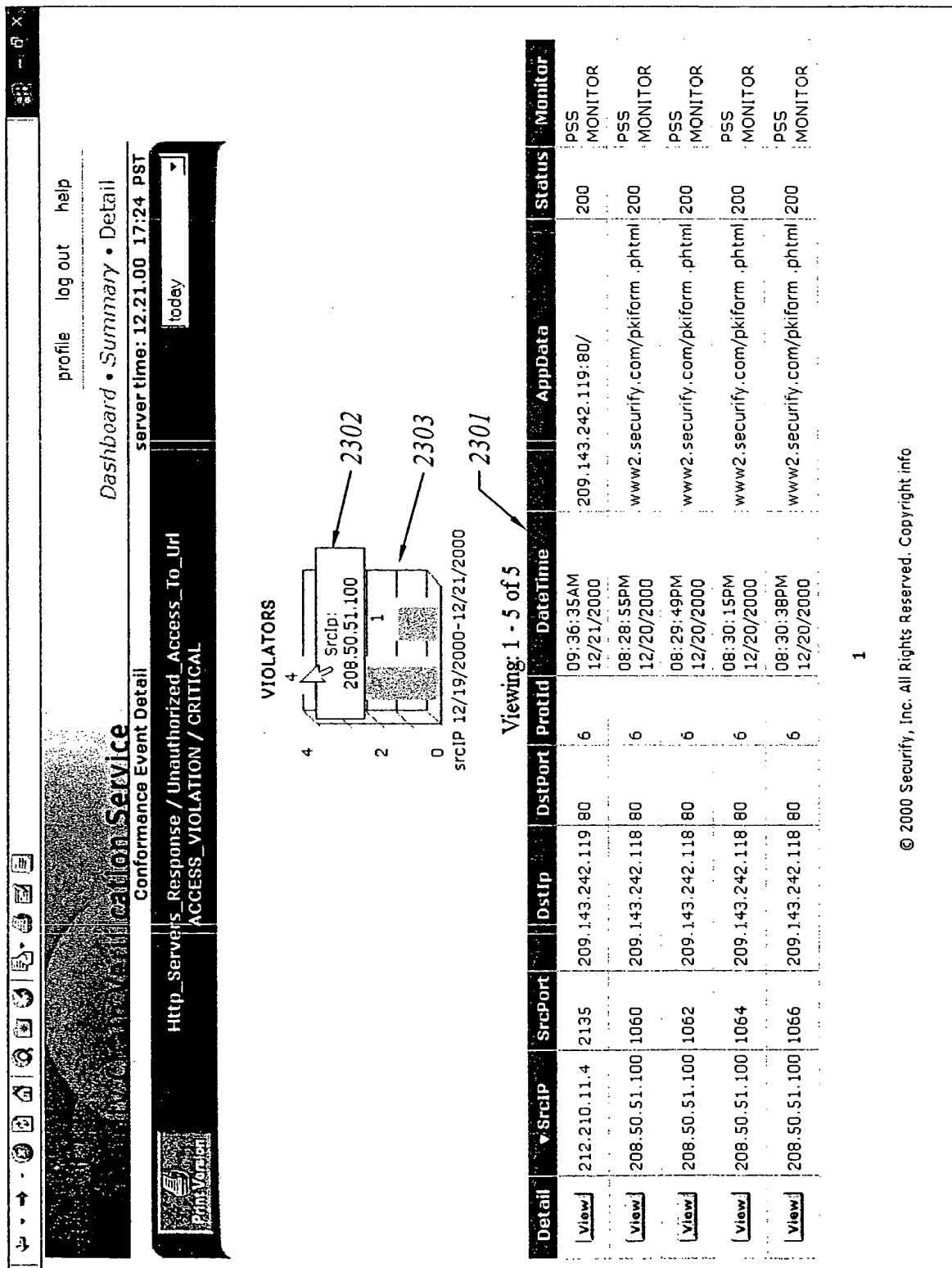




24/37

FIG. 23

BEST AVAILABLE COPY





25/37

FIG. 24

BEST AVAILABLE COPY

SVS - Protocol Event Detail - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search History Favorites Links Atlavista - Welcome CNN.com Customise Links Free Hotmail

Address C:\

profile log out help

Dashboard • Policy History

server time: 12:26:00 9:21 PST

Protocol Event Details

Http_Servers_Response / Unauthorized_Access_To_Url
ACCESS_VIOLATION / CRITICAL

Point Version

Select Protocol - Action

IP-ASSOCIATION

TCP-CONNECT

HTTP-GET

HTTP-RESPONSE

TCP-CLOSE

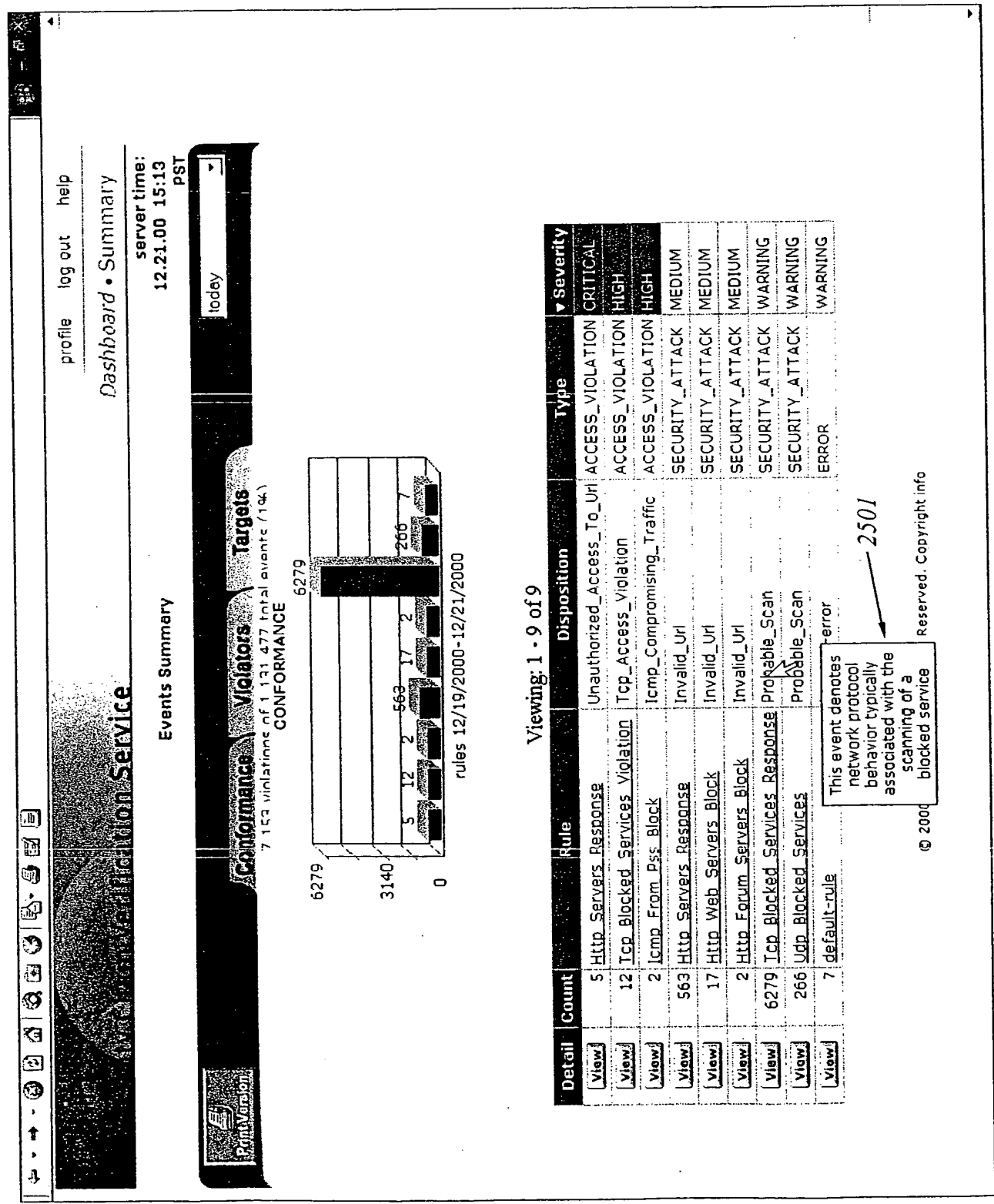
IP - ASSOCIATION	
Protocol	Target
IPAddr32	212.210.11.4 209.143.242.119
Port	2135 80
IFAddr	0003326D83C00000 0050DA16E97C0000
IpprotId	6 6

© 2000 Security, Inc. All Rights Reserved. Copyright info

javascript:MM_showHideLayers('Protocol0','show','Protocol1','hide','Protocol2','hide','Protocol3','hide','Protocol4'

FIG. 25

BEST AVAILABLE COPY





27/37

FIG. 26

BEST AVAILABLE COPY

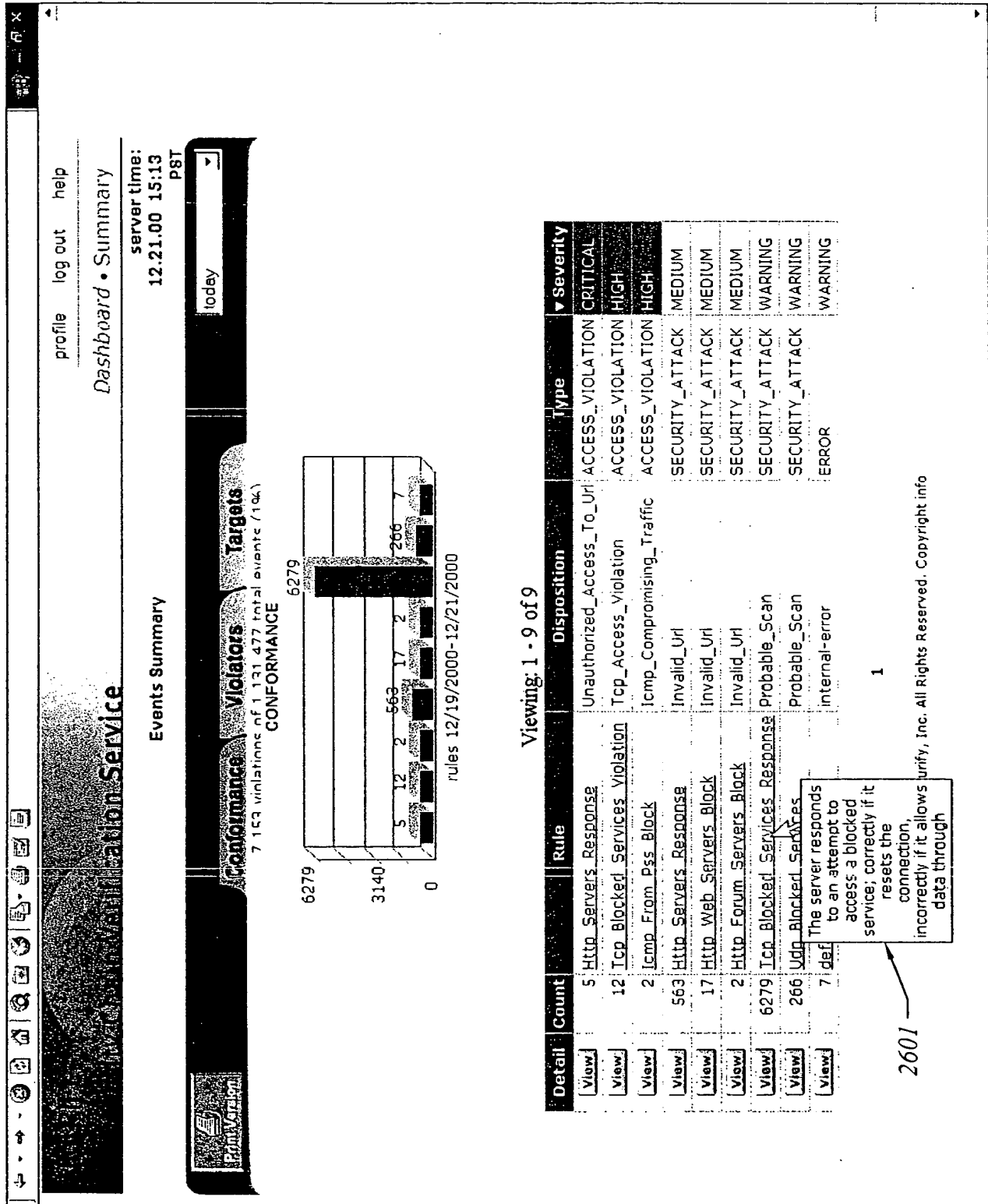
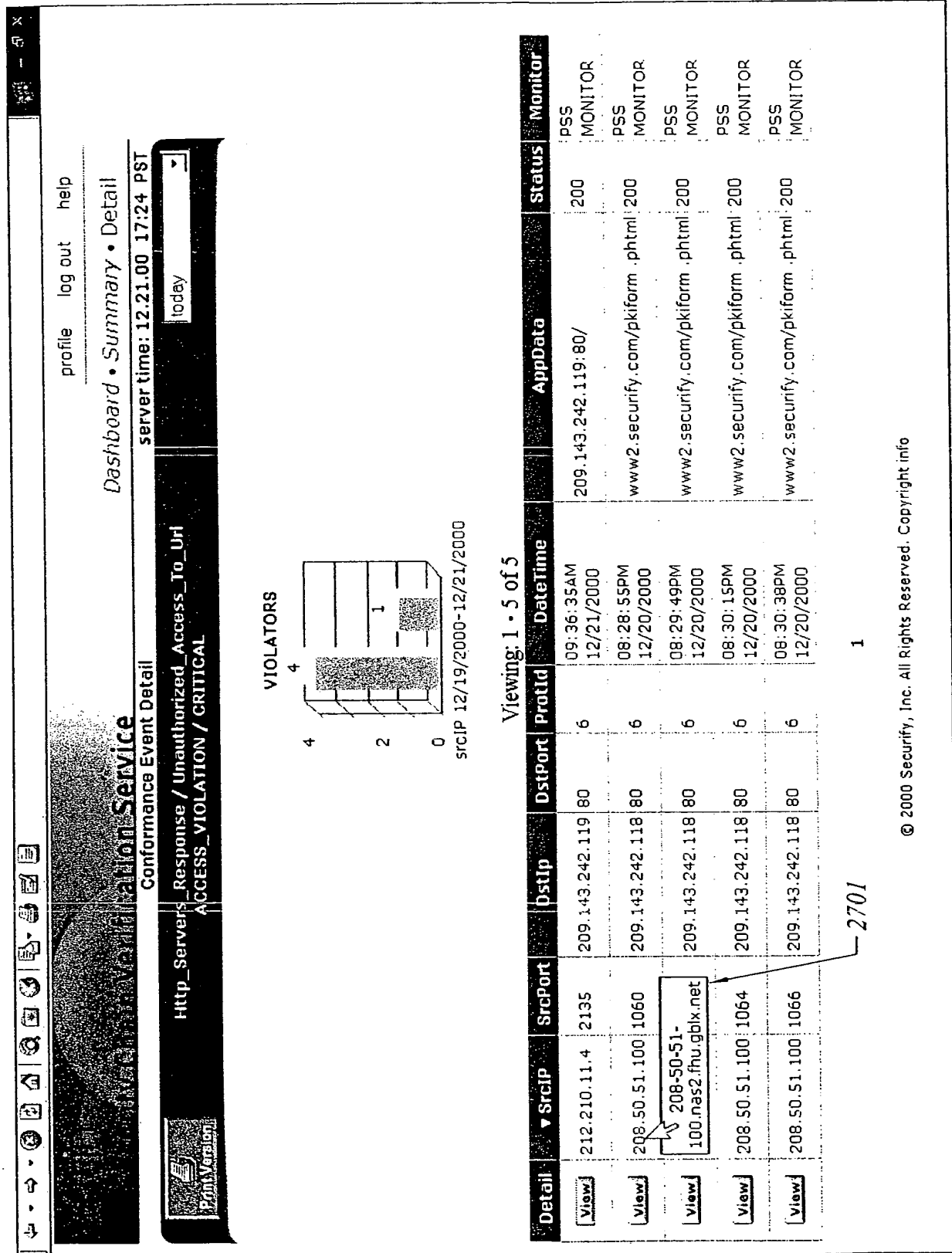


FIG. 27

28/37

BEST AVAILABLE COPY





29/37

BEST AVAILABLE COPY

Internet Explorer - Alerts - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites History

Address Bar: http://www2.xxx.com/pliform.html

profile log out help

Dashboard • Alert History

server time: 12.21.00 15:53 PST

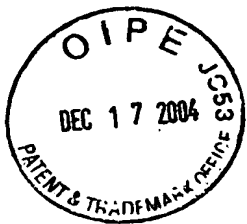
Alert History

Alert ID	Alert Time	Alert Description	Alert Type	Alert Status	Alert Action
1	08:29:49PM 12/20/2000	Unauthorized Access To URL	ACCESS VIOLATION	208.50.51.100	209.143.242.118

© 2000 Security, Inc. All Rights Reserved. Copyright info

2801

FIG. 28



30/37

BEST AVAILABLE COPY

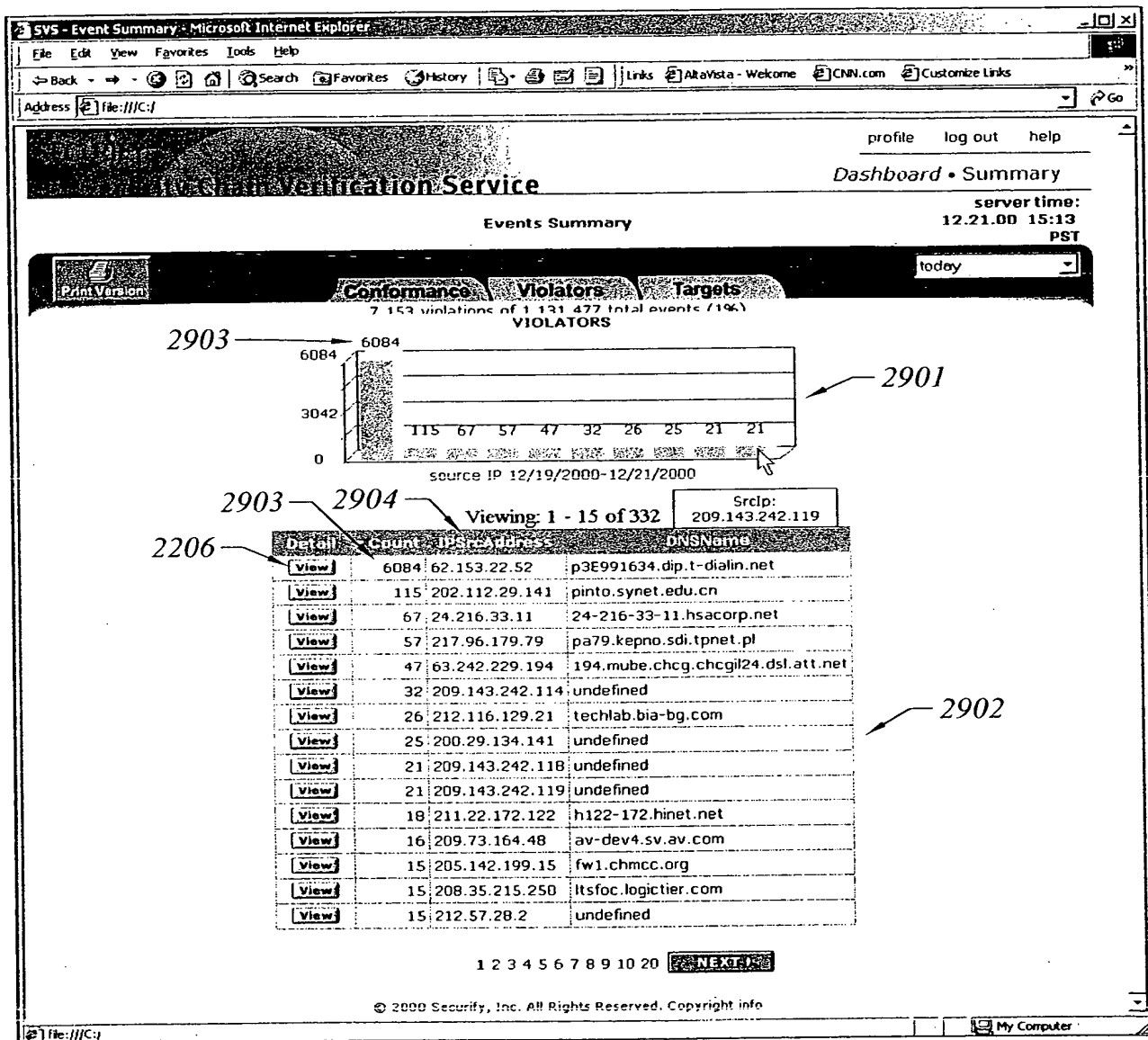


FIG. 29



31/37

BEST AVAILABLE COPY

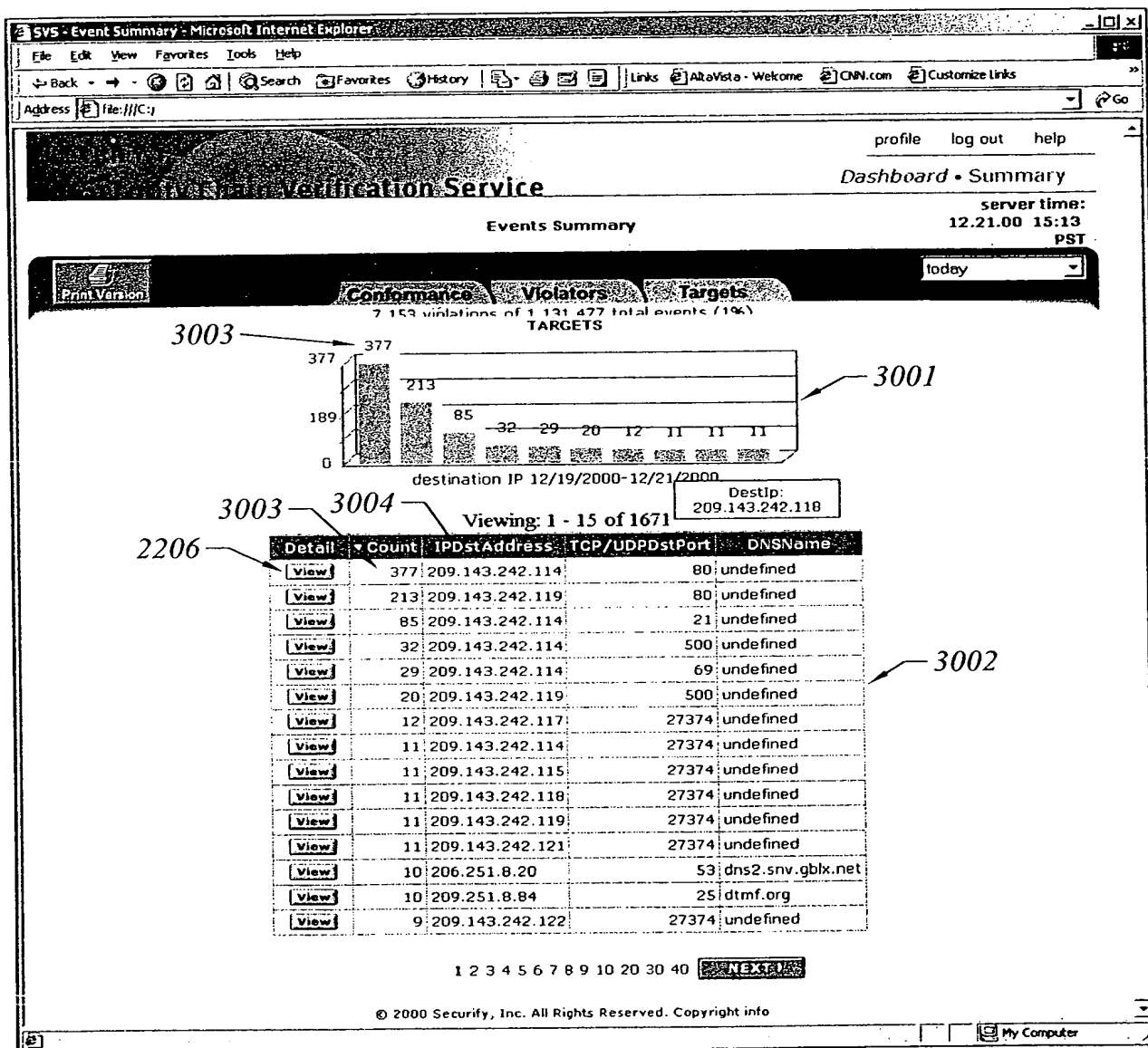


FIG. 30

Advanced Search - Microsoft Internet Explorer

Address <https://> Go

SECURIFY

[x Close](#)

Advanced Search

Filter results by One or All of the following:

Protocol

Rule

or

(regular expression in Rule)

Disposition

or

(regular expression in Disposition)

Source IP

Target IP

TargetPort

Monitor(s)
INTRANET_LOCAL_MONITOR
INTRANET_MONITOR
PARTNER_A_MONITOR

© 2000, 2001 Securify, Inc. All Rights Reserved.
Copyright info

3101

3102

3104

3103

3105

3100

3106

3106

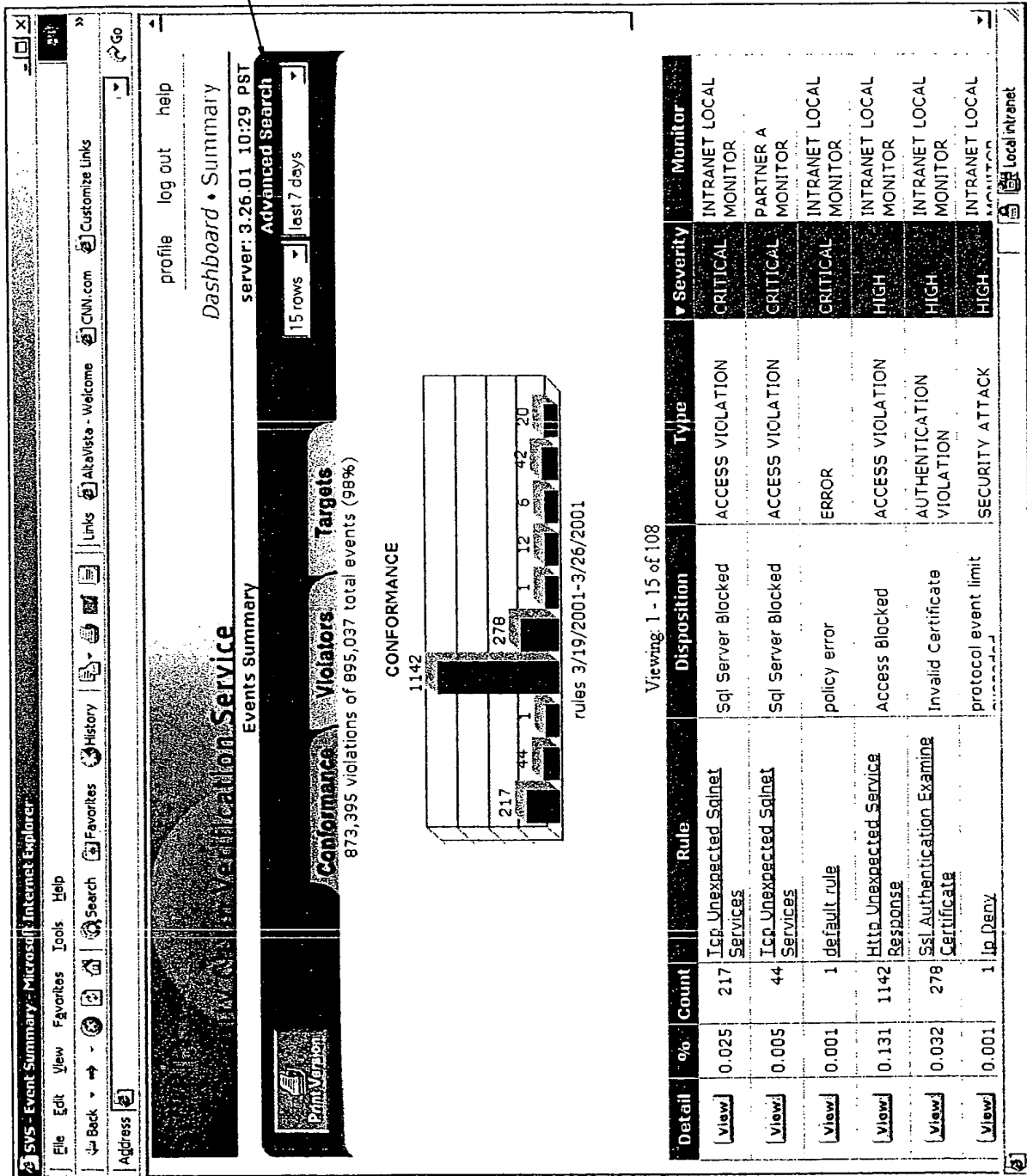
FIG. 31



33/37

BEST AVAILABLE COPY

FIG. 32



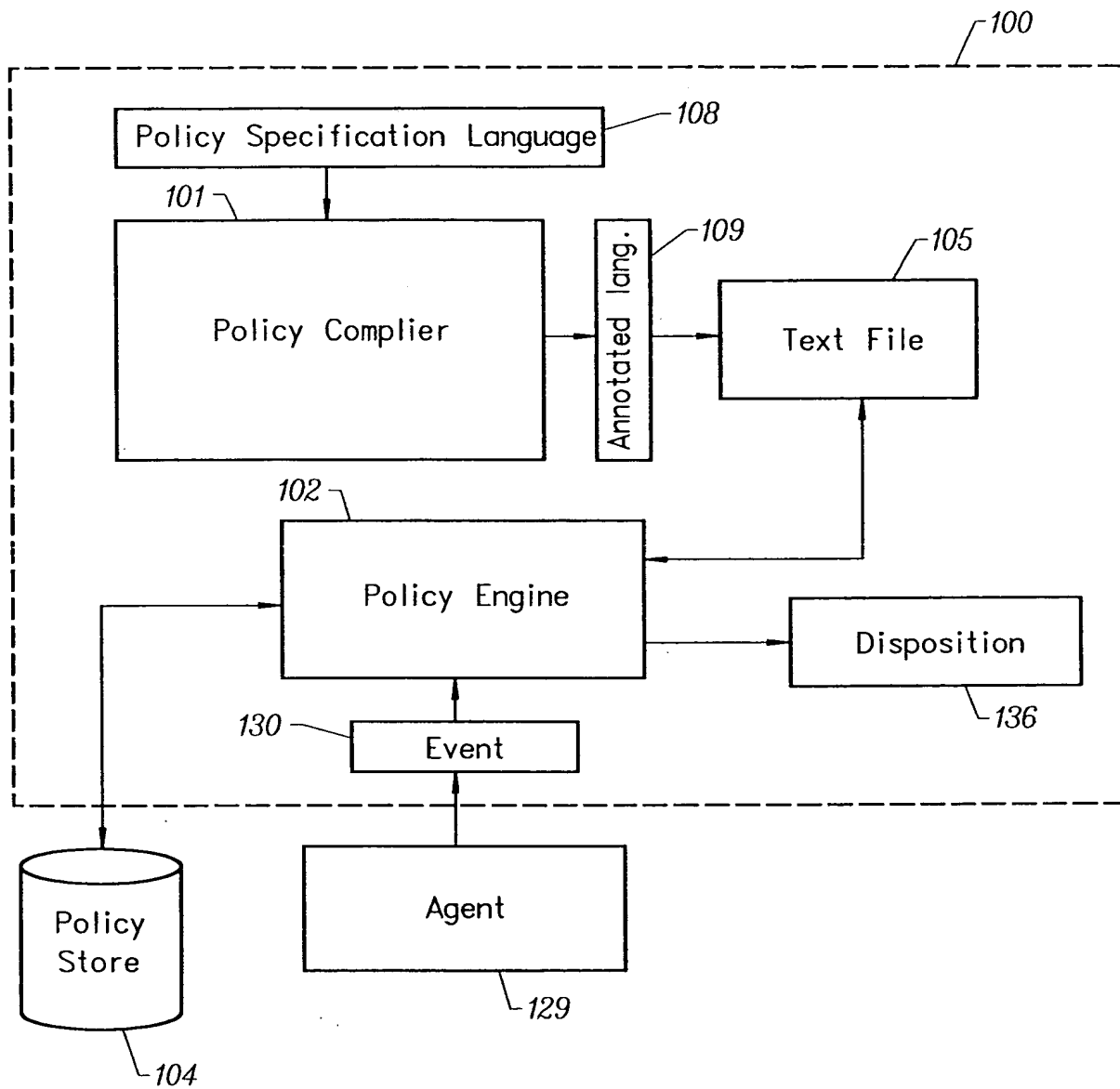


FIG. 33

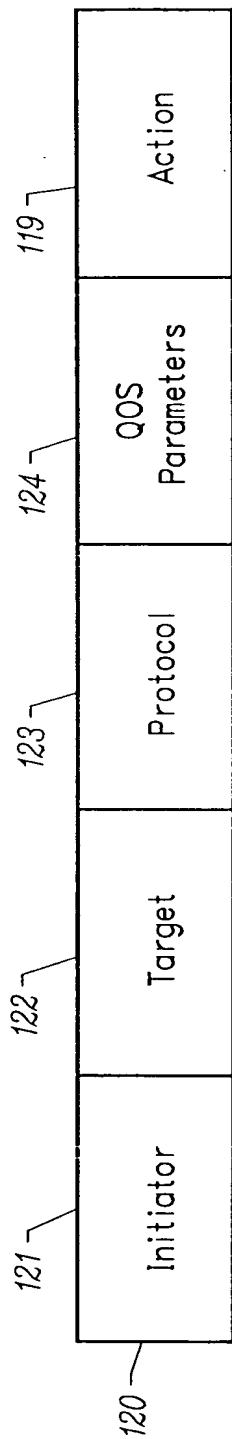


FIG. 34

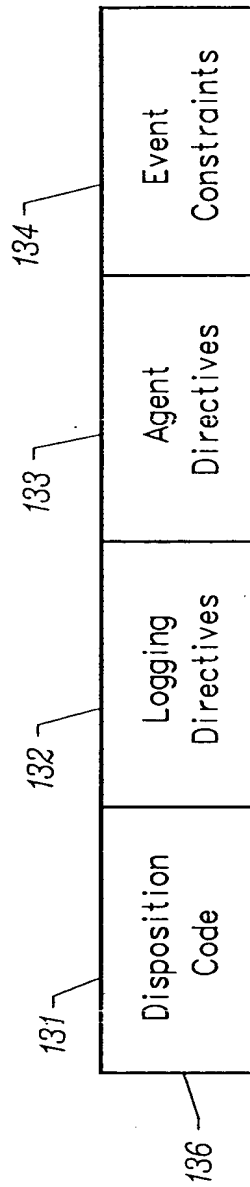


FIG. 35

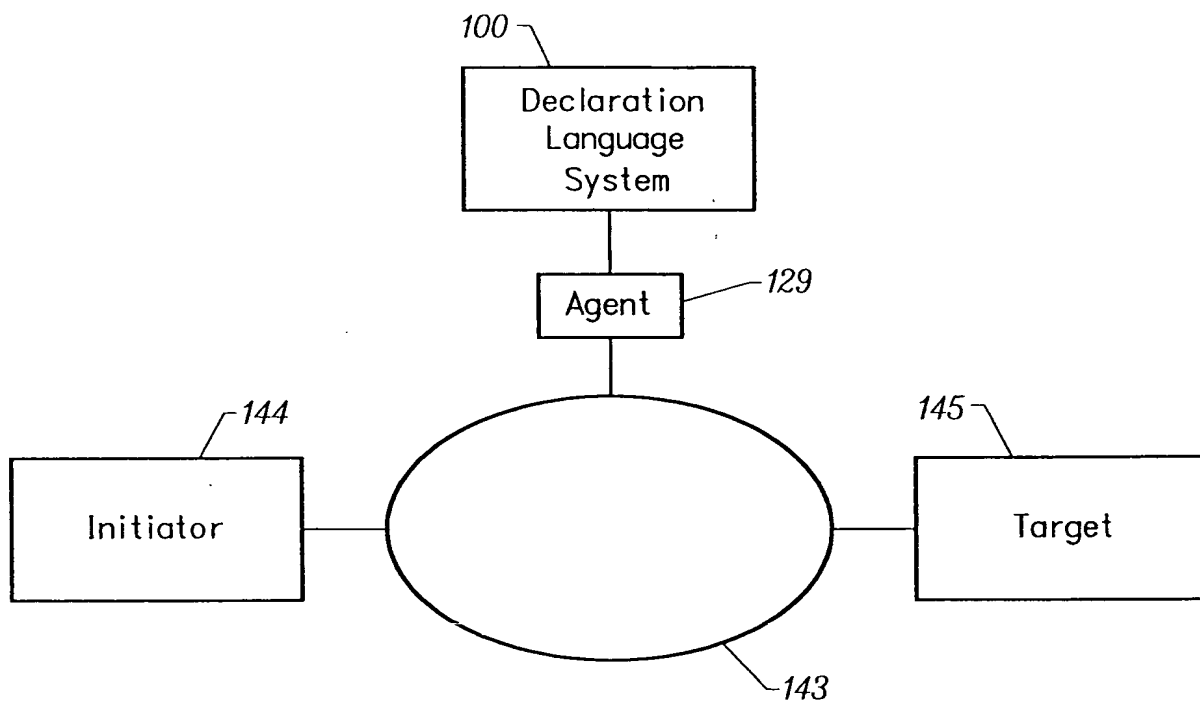


FIG. 36

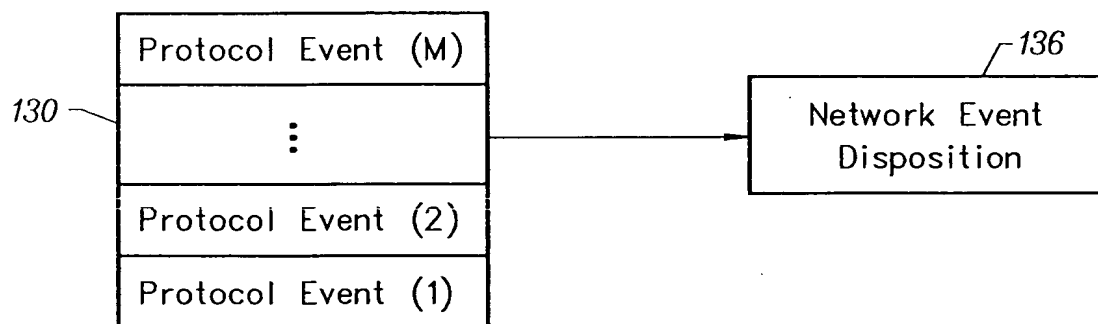


FIG. 37A

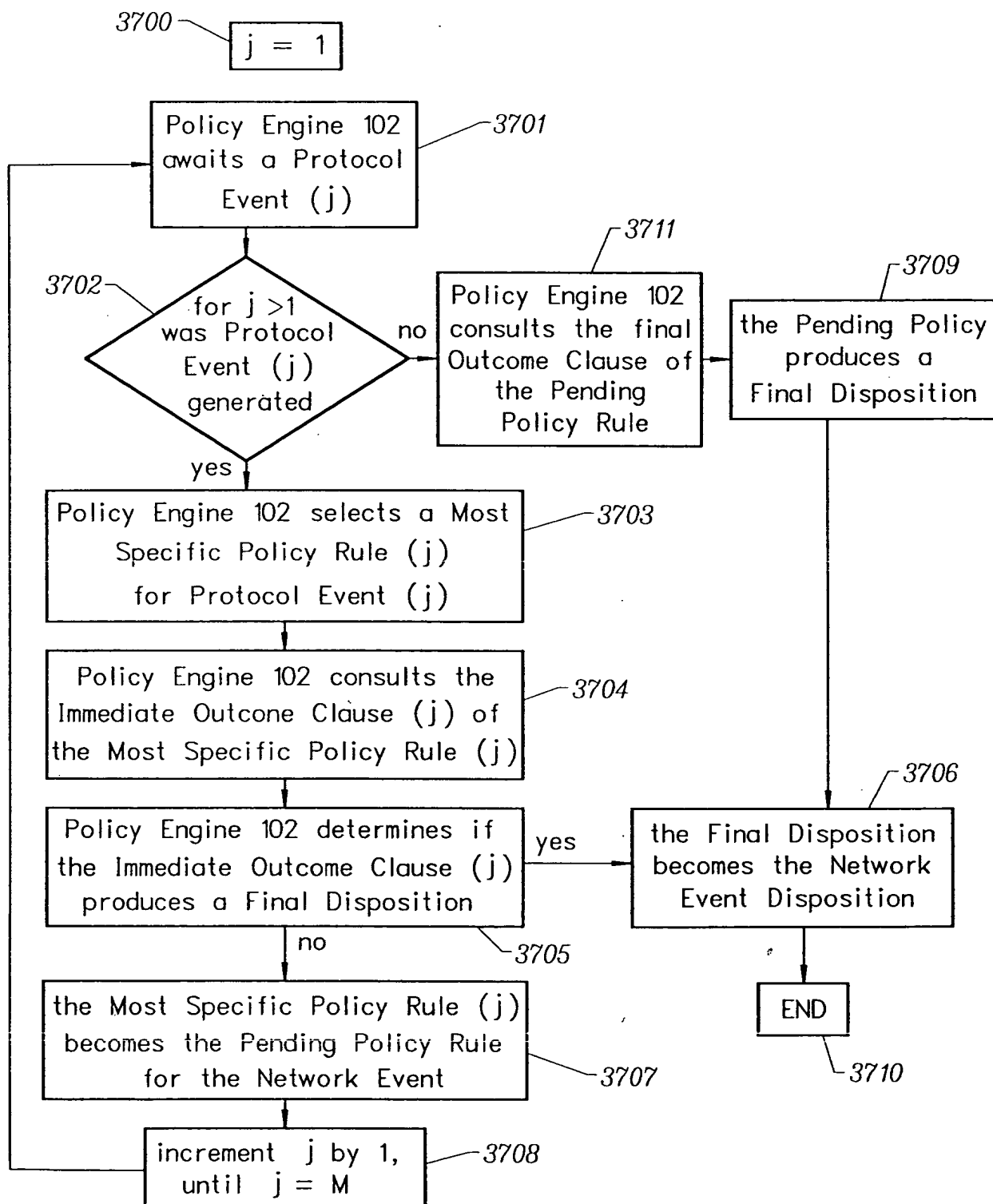


FIG. 37B